PB88-225032

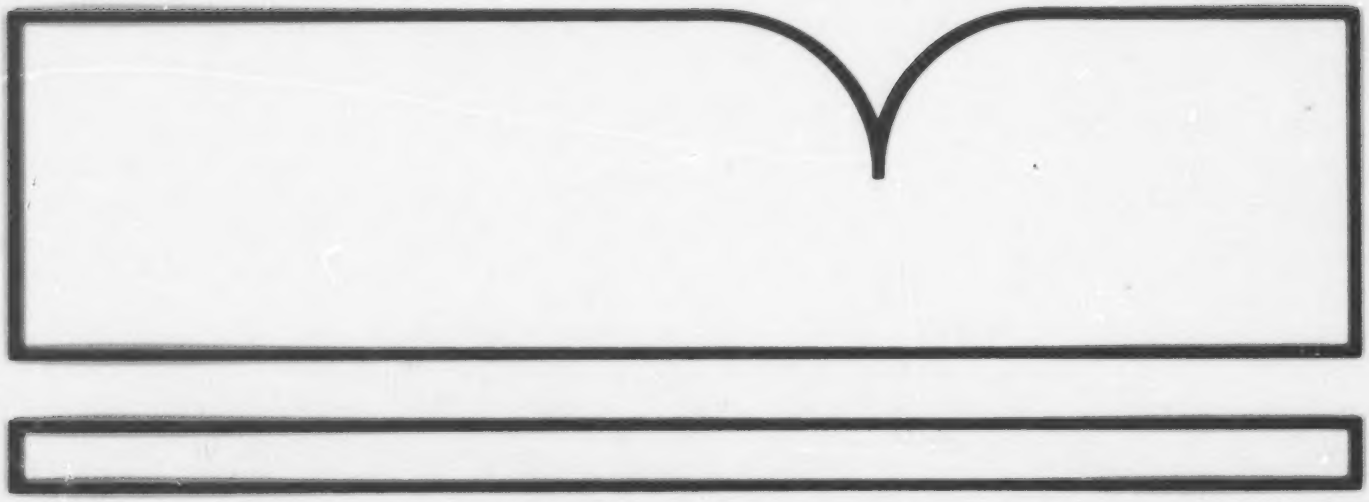
Probability and Control Cost Effectiveness for Accidental Toxic Chemical Releases

Radian Corp., Austin, TX

Prepared for

Environmental Protection Agency
Research Triangle Park, NC

Jun 88



U.S. Department of Commerce
National Technical Information Service
NTIS

PB88-225032

EPA/600/D-88/137
June 1988

PROBABILITY AND CONTROL COST EFFECTIVENESS FOR ACCIDENTAL TOXIC CHEMICAL RELEASES

Glenn B. DeWolf
Jeffrey D. Quass
Radian Corporation
8501 MoPac Boulevard
P.O. Box 201088
Austin, TX 78720-1088

and

Jane C. Bare
U.S. Environmental Protection Agency
Air and Energy Engineering Research Laboratory
Research Triangle Park, NC 27711

EPA Project Officer
Jane C. Bare

EPA Contract 68-02-3994

AIR AND ENERGY ENGINEERING RESEARCH LABORATORY
OFFICE OF RESEARCH AND DEVELOPMENT
U.S. ENVIRONMENTAL PROTECTION AGENCY
RESEARCH TRIANGLE PARK, NC 27711

REPRODUCED BY
U.S. DEPARTMENT OF COMMERCE
National Technical Information Service
SPRINGFIELD, VA. 22161

TECHNICAL REPORT DATA
(Please read Instructions on the reverse before completing)

1. REPORT NO. EPA/600/D-88/137	2.
3. RECIPIENT'S ACCESSION NO. PB88-225032/AS	
4. TITLE AND SUBTITLE Probability and Control Cost Effectiveness for Accidental Toxic Chemical Releases	5. REPORT DATE June 1988
	6. PERFORMING ORGANIZATION CODE
7. AUTHOR(S) G. B. DeWolf and J. D. Quass (Radian); and J. C. Bare (EPA/AEERL)	8. PERFORMING ORGANIZATION REPORT NO.
9. PERFORMING ORGANIZATION NAME AND ADDRESS Radian Corporation P. O. Box 201088 Austin, Texas 78720-1088	10. PROGRAM ELEMENT NO.
	11. CONTRACT/GRANT NO. 68-02-3994
12. SPONSORING AGENCY NAME AND ADDRESS EPA, Office of Research and Development Air and Energy Engineering Research Laboratory Research Triangle Park, NC 27711	13. TYPE OF REPORT AND PERIOD COVERED Published paper
	14. SPONSORING AGENCY CODE EPA/600/13

15. SUPPLEMENTARY NOTES AEERL project officer is Jane C. Bare, Mail Drop 62b, 919/541-1528.

16. ABSTRACT The paper shows how fault tree analysis (FTA) of a process system can be used to compare the relative effectiveness of various equipment, design, and operating measures for release prevention and protection applied to process streams. It also shows how the costs of various safety control measures can be estimated and combined with accident frequency estimates to provide a basis for efficiently allocating financial resources for safety. In addition to the positive aspects of the methodology shown, limitations of the methodology and needs for future investigations are highlighted. Attempting to prevent and protect against an accidental or emergency release of a toxic gas or vapor is preferable to actions taken after such a release. Planning for emergencies should include examining possibilities for reducing the chances that an accident can occur in the first place. Of the various formal, quantitative methods for estimating how releases might occur and their probability for process systems, FTA is being used more frequently. While there are current limitations to this method, due to a lack of adequate reliability data for process system components, it can still be used to provide valuable information to planners.

17. KEY WORDS AND DOCUMENT ANALYSIS

a. DESCRIPTORS	b. IDENTIFIERS/OPEN ENDED TERMS	c. COSATI Field/Group
Pollution	Pollution Control	13B 14A
Cost Effectiveness	Stationary Sources	13L
Accident Prevention	Accidental Releases	07B, 07C
Chemical Compounds	Toxic Chemicals	06T
Toxicity	Fault Tree Analysis	14G 14B
Safety	Emergencies	12A
Emission		
Analyzing		
Probability Theory		

18. DISTRIBUTION STATEMENT Release to Public	19. SECURITY CLASS (This Report) Unclassified	21. NO. OF PAGES 20
	20. SECURITY CLASS (This page) Unclassified	22. PRICE A03 12.95

EPA Form 2220-1 (9-73)

NOTICE

This document has been reviewed in accordance with U.S. Environmental Protection Agency policy and approved for publication. Mention of trade names or commercial products does not constitute endorsement or recommendation for use.

INTRODUCTION

This paper is based on technical work performed in seeking better ways to deal with the economics of accidental chemical release prevention, protection, and mitigation. It is presented by the authors to illustrate a methodology and does not constitute an endorsement of such a methodology by either Radian Corporation or the U.S. EPA. The accidental release of toxic chemicals has received increased attention since the Bhopal, India, tragedy of December 1984 when an air release of methyl isocyanate killed over 2,000 people. While this was a dramatic event of historical proportions, hazardous releases of a lesser scale occur frequently. The potential for catastrophic releases does exist. The increased attention to this issue by industry, government, and the general public is resulting in closer examination of methods for preventing such incidents.

Prevention consists of hazard identification followed by application of measures to reduce the probability that an incident will occur. Prevention measures may take many forms, from process and equipment modifications through changes in procedures and practices. It is useful to be able to evaluate the effectiveness of these measures both technically and economically so that the most benefit can be obtained for each dollar expended.

The benefit of prevention measures can be expressed as a reduction in the probability or frequency of an accidental release. The cost can be estimated by standard engineering cost estimating techniques. A cost effectiveness can be determined for each hazard control measure if the benefits and costs are known. Cost effectiveness is simply a cost-to-benefit ratio. In this paper, the costs and benefits of example control measures for preventing accidental releases are examined for a simple system. The purpose of this exercise is to

illustrate a technique which can be applied to more complex systems and might be used to better define cost effectiveness of various means of accidental release prevention.

METHODOLOGY

The frequency of an accidental release from a process system can be estimated using quantitative fault tree analysis. Probability and frequency data are drawn from the technical literature or based on engineering judgement for various system failures that could lead to an accidental release.

Since the purpose of this study is to illustrate a technique and concept, the system selected has been kept simple so as not to obscure the main concepts in a morass of detail. Before proceeding further, some fundamental concepts and definitions related to fault tree analysis are presented. A detailed discussion of fault trees is found in the technical literature, and the reader is referred to such literature for a more detailed exposition than is provided here (1, 2).

For a chemical process system, a containment failure can lead to one or more of three significant accidents if the released material has the requisite physical and chemical properties: fire, explosion, or toxic release.

In fact, any one of these events can be a cause of the others. For example, an explosion could damage a process vessel containing a toxic chemical and cause its release. A flammable material that is also toxic might escape from a small leak, ignite, and cause a fire that leads to a larger release. Or, a toxic release might cause an operator to take some action that could lead to a fire or explosion. There are, of course, a large number of potential direct and indirect causes of a release, a full discussion of which is beyond the scope of this paper. A fault tree analysis can trace a series of causes or events that lead to a release.

Fault tree analysis is a formal system of reliability and safety analysis. It is logical and well documented and can be either qualitative or quantitative. Fault tree analysis can be applied to chemical process systems to estimate the probabilities and frequencies of various kinds of system failures that lead to downtime or the realization of safety hazards such as accidental releases. There has been increasing interest in formal hazard identification and analysis techniques in recent years as both industry and government agencies have faced the issue of process safety and the prevention of accidental chemical releases to the environment. Fault tree analysis is one of these techniques.

A fault tree consists of events and pathways showing event sequences. The events are system failures or faults which may lead to other failures in an event sequence leading to a top event (final event). The sequence of events leading to a top event is an event chain. Each event may occur due to one or more preceding events or conditions. In this way, events and event

chains connect in the form of a "tree." The events that initiate or start an event chain are "primary events," and the intermediate propagating events are "enabling events." For an accidental release, the top event is a loss of containment of a flammable, explosive, or toxic material.

With each event, there is associated either a probability or frequency of failure. A frequency of failure applies to an event over a continuum of time. A probability of failure applies to an event or condition on demand. Failure frequency and probability are mathematically related. For a continuous operation, while failures are normally reported as a frequency, there is an implicit probability of failure within a given time period or mission life, where this period conceptually corresponds to the demand. For non-continuous operations, the probability of failure on demand is the fraction of demands for which the item is likely to fail. The failure frequency can be calculated, once the demand frequency is known, as the product of the demand frequency and failure probability. The demand frequency can be established directly from an operational analysis of a system, and may be related to continuous equipment or operations' failure frequencies.

Using the principles of logic trees and Boolean algebra, the probabilities and frequencies of causes can be used to calculate the probability or frequency of a succeeding event. Once a fault tree is drawn for a system and the frequency or probability of an initiating or basic event is known, the probabilities or frequencies of all succeeding events can be calculated through the top event.

At least two events, the occurrence of either of which causes a third event, constitute an "OR"-gate. At least two events, which must occur together to cause a third event, constitute an "AND"-gate. The output of an "OR"-gate is a frequency which is the sum of the frequencies of the causative events. The output of an "AND"-gate is a frequency or a probability. According to the mathematical rules, an "AND"-gate can consist of only one causative frequency. The other events must be probabilities. The output is the product of the inputs. The implications of this procedure are that each prevention, protection, or mitigation measure applied to a process system will enter the fault tree at some event and change the probability or frequency of that event, thus altering the probability or frequency of the top event. Correctly applied, such measures can reduce the probability or frequency of the top event.

Once the effect of various control measures on the probability or frequency of a top event is known, costs can be estimated and the relative cost effectiveness of various control alternatives can be determined. In this study, cost effectiveness is defined as the ratio of the total annual cost of a hazard control measure to the probability or frequency reduction achieved expressed as the number of years between failures. Total annual cost is the sum of the operating and maintenance costs for the control measure and capital recovery of the initial investment.

RESULTS

This section is organized in six parts. The example baseline system is presented and described, followed by presentation of a fault tree and a brief description of each failure event. This is followed by a discussion of example control measures that might be applied to reduce the frequency or probabilities of the failure events. Some of these control measures are selected for application to this example system. Each control measure is associated with an event on the fault tree and alters its frequency or probability. The top event frequency is recalculated after the control measures are applied. The top event frequencies for the baseline system and the system after the application of control measures are compared along with their cost effectiveness values.

Example System Description

The example process system is a disposal tank for a toxic vent gas or vapor from a chemical process. The configuration of this system, shown in Figure 1, was adapted from a system described in the technical literature (2).

A vented toxic gas stream is routed to a closed absorption system rather than to a scrubber to preclude routine discharges to the atmosphere. A holding tank is partially filled with absorption medium that is circulated by pumping through a mixing eductor where the gas dissolves and is neutralized.

A safety pressure relief valve is also provided for automatic relief if a specific set pressure is exceeded. A bypass vent valve allows manual intervention to relieve overpressure in the tank if a process upset requires it. Potential failure events which can lead to an accidental release are defined in a system fault tree with a release as the top event.

Fault Tree of Example System

The fundamental fault tree for this system is shown in Figure 2 using standard symbols defined in Reference 1. This fault tree includes a scrubber, the addition of which is discussed shortly. It is not considered part of the baseline system. For the baseline system, the top event of this study is a gas release to the atmosphere through the vent line on top of the tank. This can occur through either the bypass vent valve or the pressure relief valve.

Those events shown in circles are defined as the primary events for this case. The events with the diamond-circle symbol are pseudo-primary events. Primary events are those for which probability or frequency data are known or must be known in order to permit resolution of the fault tree. The fault tree shows the relationship between various events that can lead to a release. Secondary events are shown as rectangles.

Failure frequencies or probabilities for each primary failure were obtained from the literature or assumed values using engineering judgement They appear later in Table 1 along with results. It is important to distinguish between failure frequencies and probabilities in this study.

Frequencies are expressed as occurrences per year. A failure probability applies to events that occur on demand and is the fraction of demands for which a failure will occur. This will become clearer in the brief discussion of the various events which follows. The values of failure frequencies and probabilities are examples only and were taken from the technical literature. Such values are based on averages from industrial experience and may not represent values for all systems or industrial facilities. The ensuing discussion of the base case describes how each failure might occur and illustrates the calculation of each derived failure frequency from its causes.

Evaluation of Fault Tree

The evaluation of each event of the fault tree is explained below:

Pump Stops --

For the system to be operating, the pump must be operating. A typical failure rate for a pump is 0.26 failures/yr. (3).

Circulation Valve Closed--

The normal operating mode for the circulation valve is open. The valve could be closed, representing a failure condition, due to human error or a mechanical failure. If it is assumed that the only way human error would result in a closed valve is a failure to open it after an intended closure, then the failure rate for having an open valve is related to the frequency of closure. For purposes of this study, it is assumed that such closure occurs only when the pump needs routine servicing or fails.

If human error is assumed to be more frequent than mechanical failure for valve closure, then this will determine the failure rate for the valve. A typical probability or error per task is 10^{-2} failures/demand (4). This means that the human operator is expected to fail to open the valve once in every 100 times the operator is required to do so. The demand frequency in this case is the closure frequency calculated above, since after every closure the valve should be opened.

This analysis could be shown as a sub-fault tree for the event shown in Figure 2 as valve closed. For simplicity this has been defined as a pseudo-primary event.

The frequency of failure for the valve being closed when it should be open is the demand frequency multiplied by the probability of failure on demand. The assumed demand frequency is 0.26 failures/yr.

$0.26 \text{ demands/yr} \times 10^{-2} \text{ failures/demand} = 0.26 \times 10^{-2} \text{ failures/yr}$

No Circulation--

Circulation failure occurs when the valve fails to open or the pump fails. The frequency of circulation failure is, therefore, the sum of the frequencies of the two causes = 0.26×10^{-2} failures/yr + 0.26 failures/yr = 0.2626 failures/yr.

Process Vent Shutoff--

The system is designed to provide vent shutoff in the event of a circulation failure. For the base case, a manual vent shutoff is assumed. This shutoff depends on the operator's observations of and correct response to a circulation failure. The human probability of failure here is 10^{-2} failures/demand.

Excess Gas--

If the circulation fails, the rate of absorption will be reduced and excess gas can accumulate in the tank, unless the process vent shutoff valve is closed. The frequency of excess gas is the product of the frequency of circulation failure and the probability that the vent shutoff will not take place. A manual vent shutoff is assumed for the base case. The excess gas frequency is 0.2626 failures/yr x 10^{-2} failures/demand = 2.626 x 10^{-3} failures/yr.

Reagent Failure--

For this study, it is assumed that the baseline system relies on manual reagent makeup. Reagent failure can occur in several ways: 1) the wrong reagent or no reagent is used; 2) inadequate reagent is used; and, 3) the reagent is not replaced after it is consumed.

Each of these failures can be directly related to a human action and, therefore, a human error.

The number of demands for human intervention depends on the reagent consumption rate which depends on the rate at which toxic gas enters the system, and the system size. This hypothetical example assumes that the rate of reagent replenishment is once every 2 weeks or 52/2 = 26 times/yr which is the human intervention demand rate. The reagent failure frequency = 26 failures/yr x 10^{-2} failures/demand = 0.26 failures/yr.

Gas Not Absorbed--

In this example, the failure frequency of the gas not being absorbed is the sum of the failure frequencies for excess gas and reagent failure = 2.626 x 10^{-3} failures/yr + 0.26 failures/yr = 0.2626 failures/yr.

External Fire--

The frequency of an external fire depends on many process and site specific factors. Baseline control is a fire hose in the vicinity. To be a threat to the tank, the fire must occur close enough to the tank and be large enough to create enough heat to increase the pressure and actuate the relief valve. The failure frequency assumed for this example is 2 x 10^{-2} failures (fires)/yr.

Excess Pressure--

The frequency of excess pressure is the sum of the frequencies of external fire and gas not absorbed. The frequency of excess pressure = 2 x 10^{-2} failures/yr + 0.2626 failures/yr = 0.283 failures/yr.

Mechanical Failure of Relief Valve--

The mechanical failure of a relief valve of concern for a continuous gas release is its opening when not required to be open. This could occur due to corrosion or failure to reseat after a previous opening. Baseline controls are assumed to be some inspection, testing, and maintenance. The failure frequency for a relief valve to be open when it should be closed is taken as 0.088 failures/yr for purposes of this study (3).

Release Through Relief Valve--

This is not a functional failure of the relief valve because the valve should open under excess pressure. But it is a failure for the total process because the design intent is that releases do not occur, and the release is the culmination of a series of preceding failures. The release through the relief valve is the consequence of either the mechanical or excess pressure failure already discussed, and is, therefore, a system failure from a release perspective. The frequency of relief valve opening due to these failures is the sum of the two causes = 0.088 failures/yr + 0.283 failures/yr = 0.371 failures/yr.

Release Through Bypass--

A failure in which the bypass is open when it should be closed is attributable to human error or mechanical failure of the valve. A release through the bypass valve can occur even without excess pressure. For simplicity in this example, the bypass open failure frequency is assumed to be 0.01 failures/yr.

Gas Release--

The failure frequency of a gas release from the baseline system, without a scrubber, is the sum of the frequencies of the bypass open failure and the relief valve open failure = 0.01 failures/yr + 0.371 failures/yr = 0.381 failures/yr.

Process Hazard Control Measures

Each event of the fault tree of Figure 2 is a process hazard which can lead to an accidental release of the toxic gas near the bypass vent or relief valve. Various controls can be applied to reduce the frequency of these hazards. An obvious protection measure, applied directly to the top event hazard itself, is the addition of a scrubber to the vent outlet piping, downstream of the bypass and relief valves, to absorb and neutralize the gas. Other control measures can be introduced to counter each hazard identified in the fault tree. These measures, which lower the probability of process failures, are termed preventive measures. The quantitative effects of various control measures alone or in combination can be estimated. This provides a quantitative basis for comparing and selecting from alternatives.

Prevention and protection measures that could be applied to this system include the addition of a scrubber and enhanced operator training as examples. A terminology that distinguishes between prevention and protection measures

is preferred. Prevention measures are directed at either primary events or enabling events in the fault tree. Protection measures apply to the top event of the actual release. The scrubber is a protection measure by this definition.

Fault Tree Analysis of System with Added Hazard Controls

The addition of the scrubber alters the top of the fault tree as shown in Figure 2. The scrubber can reduce the quantity of release by its design efficiency. Since the scrubber is used only in an emergency, the demand frequency of the scrubber is the frequency with which gas would be released from the tank vent line, calculated previously as 0.381 times/year.

With the scrubber, the frequency of release is the scrubber demand frequency multiplied by probability that the scrubber will fail on demand. This probability will be due to a multitude of possible causes which could be identified in a fault tree analysis for the scrubber system. Note that to avoid a common cause of failure of electricity or reagent for the scrubber, which might initiate the failure of the process system, the scrubber would have an independent power supply and reagent for the scrubber liquor. The scrubber operation should be separate from the basic system it is designed to protect. A different power supply and different reagent makeup schedule or personnel would be used, for example. To keep things simple for this example, it is assumed that the probability for scrubber failure on demand is 0.1.

The gas release frequency is, therefore, 3.81×10^{-2} failures/yr with the scrubber. Comparison to the frequency without the scrubber clearly shows the probabilistic advantage of the scrubber, even though the scrubber system could fail when required. The scrubber has reduced the average frequency of release to the environment by a factor of 10. Stated another way, without a scrubber, a release may be expected to occur every 2.6 years. With the scrubber, a release event may be expected once every 26 years.

The effects of the other control measures are determined similarly. The absence of a control measure corresponds to a probability of failure of 1.0 for the control measure. If a control measure is added to the system in such a manner as to create an "AND"-gate, then the failure event to which the control measure applies can propagate only if the control measure fails. The frequency of propagation of the failure through the "AND"-gate is mathematically the product of the frequency of failure of the controlled failure event and the probability of failure of the control measure. An operative control measure has a probability of failure of less than 1.0. Therefore, the frequency of the propagation of the controlled failure event is reduced. This was easily seen in the addition of the emergency scrubber just discussed.

The analogous calculations with other control measures added are not repeated in their entirety here. One calculation is of particular interest, however, that for the "gas not absorbed" event.

The failure frequency of the gas not being absorbed is the sum of the failure frequencies for excess flow and reagent failure.

For the higher level controls this is,

5.24×10^{-6} failures/yr + 1.30×10^{-3} failures/yr = 1.30×10^{-3} failures/yr.

Note that, with the specific failure frequency or probability values selected for use in this paper, the lack of reagent completely masks the excess gas failure, and all the failures leading up to it. This means, for this specific case, that control of the hazards to this point should focus on preventing the reagent failure. Because this is an example problem, however, the controls previously applied are retained for the cost effectiveness analysis.

Another event of interest is the gas release itself. The failure frequency of a gas release is the sum of the frequencies of the bypass open failure and the relief valve open failure = 4.73×10^{-2} failures/yr + 5.0×10^{-3} failures/yr = 5.23×10^{-2} failures/yr. If the scrubber is included, with a failure probability of 0.1, the result is 5.23×10^{-3} failures/yr. If an enhanced scrubber is used with a reduced failure probability of 0.05, the result is 2.62×10^{-3} failures/yr.

Table 1 summarizes the results of the analyses.

Costs and Cost Effectiveness of Control Measures

Enhanced safety usually costs money. Money is limited by competition with other needs, and safety cost effectiveness is necessary. In this section, the above failure frequency estimates are combined with cost estimates to calculate the cost effectiveness of the scrubber and higher level control measures. Note that, to apply the technique illustrated in this study to a real problem, the cost of preparing the fault tree and cost effectiveness analysis would also have to be included as part of the cost.

Cost effectiveness is calculated by dividing the total annual cost of a control measure by that control measure's effectiveness as measured by the frequency reduction of an accidental release due to the control measure.

The same can be done for combinations of control measures which allows optimization of the cost effective reduction for accidental release frequency. Such optimization is outside the scope of this paper, but a comparison of several alternative combinations of control measures is provided. Before discussing cost effectiveness of a single control measure, or combinations of control measures, costs are estimated.

Cost estimates were prepared for capital investment costs, operating and maintenance costs, and total annual costs. Since these costs are for illustrative purposes only, cost data for equipment were obtained from the technical literature. Costs were first estimated for the baseline system to provide baseline costs for both the basic process and the baseline control measures for preventing an accidental release. Costs were then estimated for the higher level control measures listed in Table 2.

Capital costs were estimated using standard engineering methods and include the recurring annual operating and maintenance costs (O&M) which also consist of various direct and indirect costs. Total annual cost is the sum of the annual O&M costs and capital recovery. Capital recovery is the product of the capital recovery factor and the capital cost.

All elements of capital and O&M costs do not apply to all control measures. For example, operator training costs are treated only as annual operating costs.

Cost estimates were prepared for the baseline process system, the scrubber-added system, and the higher level control measures. The baseline system costs were calculated to show the relative cost allocatable specifically to the higher level control measures compared to the baseline system.

Overall estimated costs for release frequencies and cost effectiveness are summarized in Table 3. Capital and operating costs were estimated from equipment design criteria.

Cost effectiveness has been calculated as the total annual cost of a control measure divided by the extension of time beween failures achieved by application of the control measure. The result is expressed as dollars per year. The lower the value, the more effective is the spending for the control measure.

The results in Table 3 clearly show the effect of control measures applied to the baseline system. The effects of adding only a scrubber as protection as well as the effects of various prevention controls in addition to the scrubber are shown.

As shown in Table 3, adding the scrubber to the baseline controls increases the average interval between releases from every 2.6 years to every 26 years. The particular set of higher level controls selected here increase the interval to 19.6 years without the scrubber and 380 years with the higher level controls and an enhanced scrubber. The corresponding cost effectiveness of these controls expressed as dollars per year of release free operation ranges from $323/yr for the scrubber alone to $36/yr for the higher level controls when combined with the scrubber.

It is significant to note that, in selecting control measures, cost effectiveness alone may not be sufficient. A judgement must still be made concerning the acceptable average interval between releases. This judgement should be made as part of a total risk analysis that examines consequences, and involves the controversial issue of acceptable risk. This subject is beyond the scope of this paper.

This analysis illustrates that expenditures for appropriate controls can extend the average safe operating life of a process system. It also implies that justification of some expenditures may depend on the age of a facility and its expected operating life. An efficient allocation of resources for safety spending must take this into account.

SUMMARY AND CONCLUSIONS

An example process system and corresponding fault tree analysis have been presented which illustrate how different levels of control measures may reduce the probability of a specific accidental release. This illustration was achieved by using a quantitative fault tree analysis to predict the frequency of a specific release and the reduction in the frequency achievable by various controls.

Conclusions of this study are:

- Quantitative fault tree analysis can be applied to process systems to aid in the selection of appropriate controls to reduce the probability or frequency of accidental releases.
- Even a relatively simple system can involve a complex interaction of control, hardware, and the human factor, so that an optimum solution may not be obvious without such an analysis.
- A formal analysis of the type illustrated here allows consideration of both equipment failure and interactions between the process system and the human operators and maintenance personnel.
- A major limitation of such a quantitative analysis is the availability of comprehensive failure probability and frequency data.
- Because of limitations in the availability of data, the methodology illustrated here should be used for relative comparisons of options and sensitivity studies rather than in attempts to predict accidental release frequencies.
- A formal, structured approach to system hazard analysis provides a basis for a sensitivity analysis which could determine which elements in the fault tree structure and control measures package are most critical to meeting safety objectives.

- The type of analysis illustrated here, when combined with an analysis of consequences, can be used to evaluate costs for different levels of risk associated with accidental chemical releases.

- This methodology can be extended to more complex systems by combining computerized fault tree analysis with cost estimating and cost effectiveness calculation routines.

REFERENCES

1. Lees, F. P., Loss Prevention in the Process Industries, Vol. 1, Butterworths, London, England, 1980. pp. 197-205.

2. Prugh, R. W., Application of Fault Tree Analysis. Chemical Engineering Progress, July 1980. pp. 59-67.

3. Atallah, S., Assessing and Managing Industrial Risk. Chemical Engineering. September 8, 1980. pp. 94-103.

4. Hauptmanns, U. and H. Sastre, Safety Analysis of a Plant for the Production of Vinyl Acetate. Journal of Chemical Engineering of Japan. April 1984. pp. 165-173.

TABLE 1. RESULTS OF QUANTITATIVE FAULT TREE ANALYSIS

Failure Event	Frequency (failures/yr) or Probability (failures/demand) Baseline	Scrubber Only	Higher Level
Pump stops	2.60×10^{-1}	2.60×10^{-1}	1.30×10^{-5}
Circulation valve closed	2.60×10^{-3}	2.60×10^{-3}	1.30×10^{-3}
No circulation	2.63×10^{-1}	2.63×10^{-1}	1.31×10^{-3}
Process vent shutoff fails	1.00×10^{-2}	1.00×10^{-2}	5.24×10^{-6}
Reagent failure	2.60×10^{-1}	2.60×10^{-1}	1.30×10^{-3}
Excess gas	2.63×10^{-3}	2.63×10^{-3}	5.24×10^{-6}
Gas not absorbed	2.63×10^{-1}	2.63×10^{-1}	1.30×10^{-3}
External fire	2.00×10^{-2}	2.00×10^{-2}	2.00×10^{-3}
Excess pressure	2.83×10^{-1}	2.83×10^{-1}	3.30×10^{-3}
Mechanical failure of relief valve	8.80×10^{-2}	8.80×10^{-2}	4.40×10^{-2}
Release through relief valve	3.71×10^{-1}	3.71×10^{-1}	4.73×10^{-2}
Release through bypass	1.00×10^{-2}	1.00×10^{-2}	5.00×10^{-3}
Scrubber failure	-	1.00×10^{-1}	5.00×10^{-2}
Gas release to the environment	3.81×10^{-1}	3.81×10^{-2}	2.63×10^{-3}
Average expected time between environmental releases, years	2.6	26	380

TABLE 2. SYSTEM FAILURES AND CORRESPONDING BASELINE AND HIGHER CONTROL MEASURES USED IN COST ESTIMATES

Event	Baseline	Higher Level
Circulation valve closed	Operator training	Enhanced training
Pump stops	-	Add alarm, second pump, and operator training
Process vent shutoff fails	Operator training	Enhanced operator training
Reagent fails	Operator training	Alarm and continuous pH monitor
External fire	Fire hose in vicinity	Add fire monitor
Mechanical failure of relief valve, open	Inspection, testing, and maintenance	Enhanced inspection; testing and maintenance
Bypass open	Operator training	Enhanced training
Scrubber fails	Initial system design	Enhanced system, with increased inspection, testing, and maintenance

TABLE 3. SUMMARY OF TOTAL SYSTEM COSTS FOR BASELINE, SCRUBBER ONLY, AND HIGHER LEVEL CONTROLS

	Baseline	Scrubber Only	Higher Level[a]
Capital Cost ($)			
Equipment	114,000	134,000	142,300
Installation	49,000	58,000	61,000
Indirects	73,000	86,000	91,000
Total	236,000	278,000	294,300
O & M Cost ($/yr)			
Labor	6,000	6,000	6,000
Maintenance	8,000	9,500	10,000
Other Directs	960	1,130	1,280
Indirects	9,500	10,170	11,000
Total	24,460	26,800	28,280
Capital Recovery[b] ($/yr) (@ 10%, 10 years)	38,000	46,000	48,000
Total Annual Cost ($/yr)	62,460	72,800	76,280
Incremental Total Annual Cost	-	10,340	13,820
Release Frequency (releases/yr)	3.81×10^{-1}	3.81×10^{-2}	2.63×10^{-3}
Average Interval Between Releases (yr)	2.6	26	380
Cost Effectiveness ($/release-free yr)	-	398	36

[a] Includes scrubber
[b] Capital recovery = capital cost x capital recovery factor

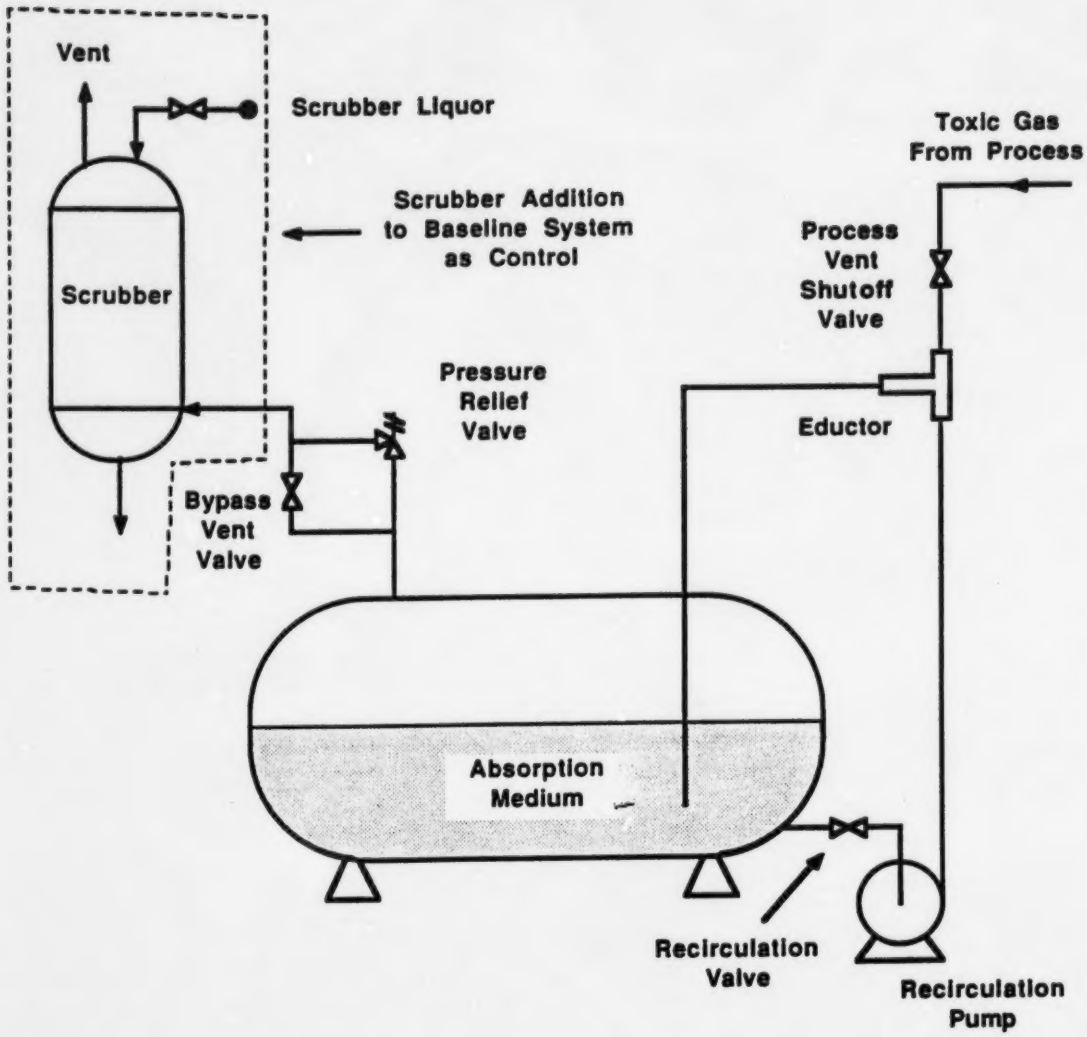


Figure 1. Example Process System for Study

Source: Adapted from Reference 2.

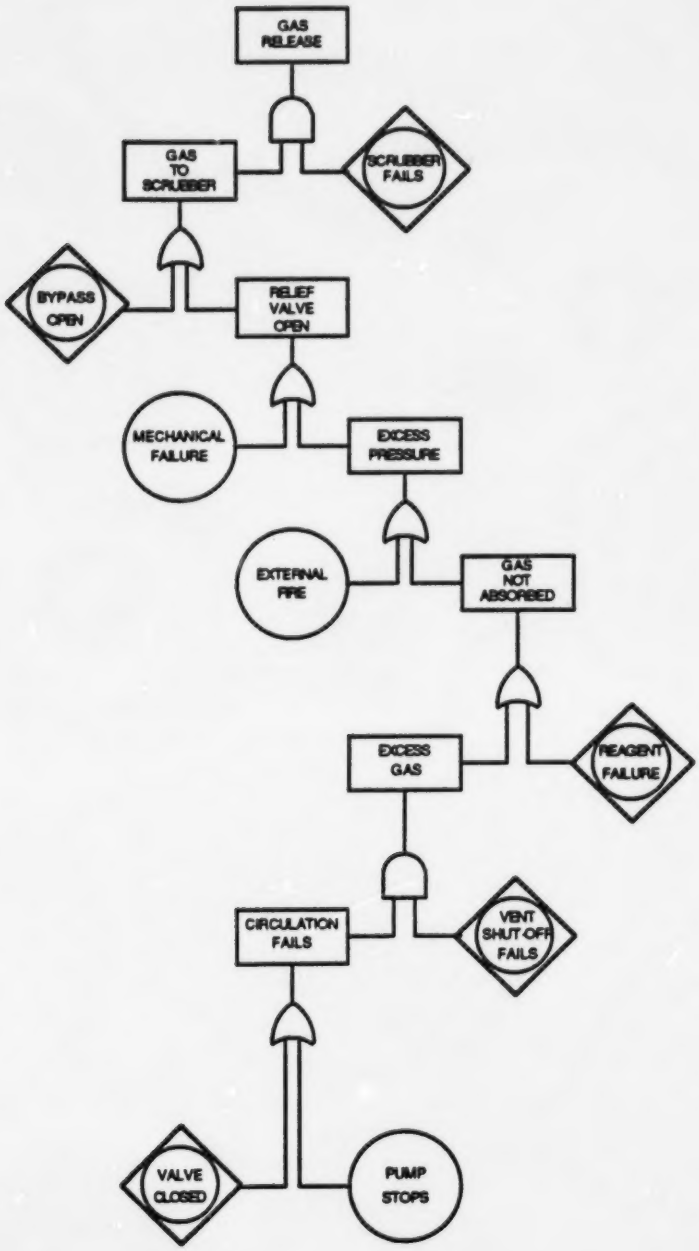


Figure 2. Fault Tree for Gas Release

Source: Adapted from Reference 2